UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/982,203	10/18/2001	Gerd Breiter	DE920010053US1	7195

7590 06/22/2006

William Kinnaman, Jr.
IBM Corporation
Intellectual Property Law Department
2455 South Road, M/S P386
Poughkeepsie, NY 12601

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 06/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/982,203	BREITER ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 7-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 7-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on June 5, 2006. Claims 1, 11, 18, 26, 28 and 30 have been amended. Claims 1-5 and 7-31 are pending.

Response to Arguments

2. Applicant's arguments filed on June 5, 2006 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-5, 7-13 and 15-17 and 30-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okamoto et al. United States Letters Patent Number 6,732,106 in view of Fung et al. United States Publication Number 2001/0052077 and in view of Arima United States Pulication Number 2002/0035516 and in view of Ginter et al. (hereinafter Ginter) U.S. Patent Number 6,948,070.

As per claims 1, 30 and 31:

Okamoto et al. teach a framework for controlling access rights to digital content in a distributed information system comprising:

first storage means for storing a reference to a user registered in said framework; (Col. 4, lines 65-67 and Col. 10, lines 14-15)

second storage means for storing a reference to digital content registered for said user; (Col. 6, lines 16-18) and,

Okamoto et al. do not explicitly disclose a third storage means for storing a reference to a digital secure repository registered for said user, the digital secure repository containing storage means for storing a unique identifier and a reference to said digital content, said digital secure repository being associated with said user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring addition authorization from an external authority.

Fung et al. in analogous art, however, disclose storage means for storing a reference to a digital secure repository registered for said user, the digital secure repository containing storage means for storing a unique identifier and a reference to said digital content. (Page 1, paragraph 8; Page 3, paragraph 36; "digital secure repository" is interpreted as "universal mobile ID": -the interpretation is given based on the similarity of the functionality of the "digital secure repository" and the "universal mobile ID")

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. to

include storage means for storing a reference to a digital secure repository registered for said user, the digital secure repository containing storage means for storing a unique identifier and a reference to said digital content. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Fung et al. (Page 5, paragraph 7) in order to prevent an authorized user from transferring to non-authorized users a key or other embodiments of a right that would allow the non-authorized users to access the for-pay content.

Both references do not explicitly disclose a digital secure repository being associated with said user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring addition authorization from an external authority.

Arima in analogous art, however discloses a storing unit that is being associated with said user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring addition authorization from an external authority. (Page 3, paragraph 30; Page 4, paragraph 46)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al.

and Fung et al. to include a digital secure repository being associated with said user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring addition authorization from an external authority. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Arima (Abstract) in order to create a storing unit to store the digital contents ordered by a customer and creating a list for transmission to a player terminal and a transmitter that sends content selected by a customer to another player terminal. This way, the digital content is accessed by authorized customer and is transmitted to one or more player terminals registered as authorized terminals.

In addition, Arima further discloses a sales center server has a storage for storing information on the website accessed by the user terminal and information on digital contents. The sales center has a function of accepting a purchase request for digital contents from the user and accessing the server having the customer's digital contents rack as a delivery destination. (Page 3, paragraph 32)

None of the references explicitly disclose a digital secure repository being accessible to said user independently of said provider. Ginter in analogous art, however, discloses a digital secure repository being accessible to said user independently of said provider. (Col. 33, lines 10-15) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the

method disclosed by Okamoto, Fung and Arima with Ginter in order to have a virtual distribution system that may be used to protect rights of various participants in electronic commerce or other electronic facilitated transactions. (Abstract; Ginter)

As per claim 2:

The combination of Okamoto, Fung, Arima and Ginter teaches all the subject matter as discussed above. In addition, Okamoto et al. further disclose a framework comprising: fourth storage means for storing a reference to an authorized rendering device registered for said user. (Col. 4, lines 60-65)

As per claim 3:

The combination of Okamoto, Fung, Arima and Ginter teaches all the subject matter as discussed above. In addition, Fung et al. further disclose a framework comprising: a communication link for establishing communication to one or more of the set of said secure repository and said rendering device. (Page 1, paragraph 8, ...each client is associated with a universal mobile ID...)

As per claim 4:

The combination of Okamoto, Fung, Arima and Ginter teaches all the subject matter as discussed above. In addition, Fung et al. further disclose a framework wherein said secure repository further comprises storage means for storing a digital key for decrypting said digital content. (Page 4, paragraph 53 and Page 5, paragraph 54)

As per claim 5:

The combination of Okamoto et al., Fung et al. and Arima teaches all the subject matter as discussed above. In addition, Fung et al. further disclose a framework wherein

said secure repository further comprises storage means for storing said list of authorized rendering device. (Page 1, paragraph 8)

As per claim 7:

The combination of Okamoto, Fung, Arima and Ginter teaches all the subject matter as discussed above. In addition, Fung et al. further disclose a framework wherein said secure repository further comprises storage means for storing a reference to said user. (Page 1, paragraph 8)

As per claim 8:

The combination of Okamoto, Fung, Arima and Ginter teaches all the subject matter as discussed above. In addition, Fung et al. further disclose a framework wherein said secure repository further comprises a communication link for establishing communication to one or more of the set of said framework and said an authorized rendering device. (Page 1, paragraph 8; ...each client is associated with a universal mobile ID... ; Page 2, paragraph 15)

As per claim 9:

The combination of Okamoto, Fung, Arima and Ginter teaches all the subject matter as discussed above. In addition, Okamoto et al. further disclose a framework wherein the framework is realized as a set of web applications forming an Internet web site. (Col. 9, lines 42-43 and Col. 11, lines 16-18)

As per claim 10:

The combination of Okamoto, Fung, Arima and Ginter teaches all the subject matter as discussed above. In addition, Okamoto et al. further disclose an Internet web

site offering a framework for controlling access rights to digital content in a distributed information system. (Col. 9, lines 44-47)

As per claims 11 and 17:

Okamoto et al. teach a method for controlling access rights to digital content in a distributed information system comprising the steps of:

registering a user with a framework for controlling access rights to digital content in said distributed information system; (Col. 12, lines 42-46)

registering digital content for said user. (Col. 13, lines 38-41)

Okamoto et al. do not explicitly disclose a digital secure repository being associated with said user independently of a particular device, said digital secure repository storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content; and controlling the rendering of said digital content in accordance with the access rights to said digital content and the list of authorized rendering devices stored in said digital secure repository so as to allow said user to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository requiring additional authorization from an external authority.

Fung et al. in analogous art, however, disclose registering a digital secure repository and digital content registered for said user for storing access rights to said digital content granted to said user by a provider and controlling the rendering of said digital content in accordance with the access rights to said digital content. (Page 1,

paragraph 8; Page 2, Paragraph 15; Page 3, paragraph 36; "digital secure repository" is interpreted as "universal mobile ID": -the interpretation is given based on the similarity of the functionality of the "digital secure repository" and the "universal mobile ID")

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. to include registering a digital secure repository and digital content registered for said user for storing access rights to said digital content granted to said user by a provider and controlling the rendering of said digital content in accordance with the access rights to said digital content. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Fung et al. (Page 5, paragraph 7) in order to prevent an authorized user from transferring to non-authorized users a key or other embodiments of a right that would allow the non-authorized users to access the for-pay content.

Both references do not explicitly disclose a digital secure repository being associated with said user independently of a particular device, a list of authorized rendering devices on which said user is allowed to render said digital content; and controlling the rendering of said digital content in accordance with the access rights to said digital content and the list of authorized rendering devices stored in said digital secure repository so as to allow said user to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring additional authorization from an external authority.

Arima in analogous art, however discloses a storing unit that is being associated with said user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring addition authorization from an external authority. (Page 3, paragraph 30; Page 4, paragraph 46)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. and Fung et al. to include a digital secure repository being associated with said user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring addition authorization from an external authority. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Arima (Abstract) in order to create a storing unit to store the digital contents ordered by a customer and creating a list for transmission to a player terminal and a transmitter that sends content selected by a customer to another player terminal. This way, the digital content is accessed by authorized customer and is transmitted to one or more player terminals registered as authorized terminals.

In addition, Arima further discloses a sales center server has a storage for storing information on the website accessed by the user terminal and information on digital contents. The sales center has a function of accepting a purchase request for digital contents from the user and accessing the server having the customer's digital contents rack as a delivery destination. (Page 3, paragraph 32)

None of the references explicitly disclose a digital secure repository being accessible to said user independently of said provider. Ginter in analogous art, however, discloses a digital secure repository being accessible to said user independently of said provider. (Col. 33, lines 10-15) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Okamoto, Fung and Arima with Ginter in order to have a virtual distribution system that may be used to protect rights of various participants in electronic commerce or other electronic facilitated transactions. (Abstract; Ginter)

As per claim 12:

The combination of Okamoto, Fung, Arima and Ginter teaches all the subject matter as discussed above. In addition, Okamato et al. further disclose a method wherein registering a user further comprises the steps of: storing a reference to said user. (Col. 12, lines 65-67)

Fung et al. further disclose a method wherein registering a user further comprises the steps of:

receiving a message from said user comprising a reference to said digital secure repository; (Page 2, paragraph 15; ...a user accesses server content by first issuing a request to the server along with his UMID.)

validating said reference to said digital secure repository; (Page 2, paragraph 15)

As per claim 13:

The combination of Okamoto et al., Fung et al. and Arima teaches all the subject matter as discussed above. In addition, Okamoto et al. further disclose a method wherein registering a digital secure repository further comprises the steps of:

storing a reference to said issued digital secure repository and sending it to the user. (Col. 17, lines 14-15)

Fung et al. further disclose a method wherein registering a digital secure repository further comprises the steps of:

receiving a message from said user comprising credentials of the user; (Page 4, paragraph 45)

validating said credentials; and (Page 4, paragraph 45)

if the credentials are valid, issuing a new digital secure repository; (Page 4, paragraph 45) and

As per claim 15:

The combination of Okamoto, Fung, Arima and Ginter teaches all the subject matter as discussed above. In addition, Arima further disclose a method comprising the step of registering an authorized rendering device for said user. (Page 3, paragraph 20)

As per claim 16:

The combination of Okamoto, Fung, Arima and Ginter teaches all the subject matter as discussed above. In addition, Okamoto et al. further disclose a method wherein registering a rendering device further comprises the steps of:

receiving a message from said user comprising credentials of the user and a reference to said rendering device to be registered; (Col. 12, lines 6-8 and Col. 4, lines 62-65)

validating said credentials; (Col. 17, lines 54-56)

if the credentials are valid, storing the reference of the rendering device associated with said user. (Col. 10, lines 15-17)

5. Claims 14 and 18-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okamoto et al. United States Letters Patent Number 6,732,106 in view of Fung et al. United States Publication Number 2001/0052077 and in view of Arima Japanese Patent No. 286621/2000 and in view of Ginter et al. (hereinafter Ginter) U.S. Patent Number 6,948,070 and further in view of Olson et al. United States Publication Number US 2002/0003878.

As per claim 14:

The combination of Okamoto, Fung, Arima and Ginter teaches all the subject matter as discussed above. In addition, Fung et al. further disclose a method wherein registering digital content further comprises the steps of:

receiving a message from said user comprising an order request and a reference to the digital secure repository registered for said user; (Page 2, paragraph 15; ...a user accesses server content by first issuing a request to the server along with his UMID.)

validating said reference; and (Page 2, paragraph 15)

if the reference is valid, performing purchase formalities; (Page 2, paragraph 15)

returning the encrypted document encryption key to the user and registering the purchased digital content for said user. (Page 2, paragraph 15)

None of the references, however, explicitly disclose encrypting the document encryption key associated with the requested digital content with the public key associated with said digital secure repository.

Olsen et al. in analogous art, however, disclose encrypting the document encryption key associated with the requested digital content with the public key associated with said digital secure repository. (Page 4, paragraph 54; ...a public key system is used to cipher the video decryption keys, ...)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al., Fung et al., Arima and Ginter to include encrypting the document encryption key associated with the requested digital content with the public key associated with said digital secure repository. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Olsen et al. (Page 5, paragraph 55) in order to protect the keys during transmission from Content Distribution Portal to the Rendering Device.

As per claims 18 and 25:

Okamoto et al. teach a method for rendering digital content on a rendering device comprising the steps of:

receiving a request for rendering digital content in a predetermined form;(Col.6 , lines 25-27)

reading information about access rights granted; (Col. 6, lines 28-35)

decrypting the document encryption key with the private key associated with said rendering device; (Col. 3, lines 57-58)

decrypting said digital content with said document encryption key; and rendering said digital content in the requested form. (Col. 2, lines 4-5 and Col. 3, line 61)

Okamoto et al. do not explicitly disclose a digital secure repository being associated with said user independently of a particular device, said digital secure repository storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content; and rendering said digital content in the requested from so as to allow said user to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository requiring additional authorization from an external authority.

Fung et al. in analogous art, however, disclose registering a digital secure repository registered for said user. (Page 2, Paragraph 15)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. to include storage means for storing a reference to a digital secure repository registered for said user, the digital secure repository containing storage means for storing a unique identifier and a reference to said digital content. This modification would have been

obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Fung et al. (Page 5, paragraph 7) in order to prevent an authorized user from transferring to non-authorized users a key or other embodiments of a right that would allow the non-authorized users to access the for-pay content.

Both references do not explicitly disclose a storing unit that is being associated with said user independently of a particular device, said digital secure repository storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content; and rendering said digital content in the requested from so as to allow said user to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository requiring additional authorization from an external authority.

Arima in analogous art, however discloses a storing unit that is being associated with said user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring addition authorization from an external authority. (Page 3, paragraph 30; Page 4, paragraph 46)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. and Fung et al. to include a digital secure repository being associated with said user

independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring addition authorization from an external authority. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Arima (Abstract) in order to create a storing unit to store the digital contents ordered by a customer and creating a list for transmission to a player terminal and a transmitter that sends content selected by a customer to another player terminal. This way, the digital content is accessed by authorized customer and is transmitted to one or more player terminals registered as authorized terminals.

In addition, Arima further discloses a sales center server has a storage for storing information on the website accessed by the user terminal and information on digital contents. The sales center has a function of accepting a purchase request for digital contents from the user and accessing the server having the customer's digital contents rack as a delivery destination. (Page 3, paragraph 32)

None of the references explicitly disclose a digital secure repository being accessible to said user independently of said provider. Ginter in analogous art, however, discloses a digital secure repository being accessible to said user independently of said provider. (Col. 33, lines 10-15) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Okamoto, Fung and Arima with Ginter in order to have a virtual

distribution system that may be used to protect rights of various participants in electronic commerce or other electronic facilitated transactions. (Abstract; Ginter)

None of the references, however, explicitly disclose getting a document encryption key encrypted with the public key associated with said rendering device. Olsen et al. in analogous art, however, disclose getting a document encryption key encrypted with the public key associated with said rendering device. (Page 4, paragraph 54; ...a public key system is used to cipher the video decryption keys, ...) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. Fung et al., Arima and Ginter to include encrypting the document encryption key associated with the requested digital content with the public key associated with said digital secure repository. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Olsen et al. (Page 5, paragraph 55) in order to protect the keys during transmission from Content distribution server to the rendering device.

As per claim 19:

The combination of Okamoto et al., Fung et al., Arima, Ginter and Olsen et al. teach all the subject matter as discussed above. In addition, Okamoto et al. further disclose a method wherein the step of getting a document encryption key further comprises the steps:

determining from a storage device associated with said rendering device whether or not the digital content is bound to said rendering device and if yes receiving said document encryption key from said storage device. (Col. 6, lines 48 and lines 56-57)

As per claim 20:

The combination of Okamoto et al., Fung et al., Arima, Ginter and Olsen et al. teach all the subject matter as discussed above. In addition, Fung et al. further disclose a method wherein the step of getting a document encryption key further comprises the step of receiving said document encryption key from a digital secure repository. (Page 2, paragraph 15;...The user then decrypts the encrypted content using both his secret PIN and the content-specific key...)

As per claim 21:

The combination of Okamoto et al., Fung et al., Arima, Ginter and Olsen et al. teach all the subject matter as discussed above. In addition, Fung et al. further disclose a method wherein the step of reading from a digital secure repository further comprises the step of communicating with said digital secure repository over a communication link. (Page 1, paragraph 8, ...each client is associated with a universal mobile ID...)

As per claim 22:

The combination of Okamoto et al., Fung et al., Arima, Ginter and Olsen et al. teach all the subject matter as discussed above. In addition, Fung et al. further disclose a method wherein the step of reading from a digital secure repository further comprises the step of retrieving said digital secure repository from a storage device also keeping said digital content. (Page 4, paragraph 46)

As per claim 23:

The combination of Okamoto et al., Fung et al., Arima, Ginter and Olsen et al. teach all the subject matter as discussed above. In addition, Okamoto et al. further disclose a method wherein the step of decrypting said digital content further comprises the step of retrieving said digital content from a storage device. (Col. 2, lines 4-5 and Col. 3, line 61)

As per claim 24:

The combination of Okamoto et al., Fung et al., Arima, Ginter and Olsen et al. teach all the subject matter as discussed above. In addition, Okamoto et al. further disclose a method wherein the step of decrypting said digital content further comprises the step of retrieving said digital content from over a communication link as downloaded or streaming data. (Col. 9, lines 50-58)

As per claim 26 and 27:

Okamoto et al. a method for binding digital content to a rendering device, the method comprising the following steps:

if binding is allowed according to the rights stored in said digital secure repository, receiving the respective document encryption key encrypted with the rendering device's public key, and storing the encrypted key for later decrypting the respective digital content. (Col. 6, lines 49-51 and Col. 6, line 55)

Okamoto et al. further disclose a communication means between the distribution server and the user device and checking distribution condition by comparing the number of digital data; of which the same consumer registered in the history data is authorized

to receive the distribution, and the distribution condition information. (Col. 6, lines 28-35). In addition, Okamoto et al. teaches encrypting means for encrypting the decryption key using a key that is created based on the media ID received from the user device.

Okamato et al. do not explicitly disclose establishing a connection from said rendering device to a digital secure repository, said digital secure repository being associated with a user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content so as to allow said user to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring additional authorization from an external authority; and requesting from said digital secure repository digital content rights for specified digital content; and document encryption key encrypted with the rendering device's public key.

Fung et al. in analogous art, however, disclose

establishing a connection from said rendering device to a digital secure repository; (Page 1, paragraph 8, ...each client is associated with a universal mobile ID...)

requesting from said digital secure repository access rights for specified digital content. (Page 2, paragraph 15)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. to include establishing a connection from said rendering device to a digital secure

repository; requesting from said digital secure repository digital content rights for specified digital content. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Fung et al. (Page 2, paragraph 14) in order to assemble the digital material which is send to the client device by using the access information which is contained in the Universal Mobile ID.

Both references do not explicitly disclose a digital secure repository being associated with said user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content so as to allow said user to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring additional authorization from an external authority.

Arima in analogous art, however discloses a storing unit that is being associated with said user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring addition authorization from an external authority. (Page 3, paragraph 30; Page 4, paragraph 46)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al.

and Fung et al. to include a digital secure repository being associated with said user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring addition authorization from an external authority. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Arima (Abstract) in order to create a storing unit to store the digital contents ordered by a customer and creating a list for transmission to a player terminal and a transmitter that sends content selected by a customer to another player terminal. This way, the digital content is accessed by authorized customer and is transmitted to one or more player terminals registered as authorized terminals.

In addition, Arima further discloses a sales center server has a storage for storing information on the website accessed by the user terminal and information on digital contents. The sales center has a function of accepting a purchase request for digital contents from the user and accessing the server having the customer's digital contents rack as a delivery destination. (Page 3, paragraph 32)

None of the references explicitly disclose a digital secure repository being accessible to said user independently of said provider. Ginter in analogous art, however, discloses a digital secure repository being accessible to said user independently of said provider. (Col. 33, lines 10-15) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the

method disclosed by Okamoto, Fung and Arima with Ginter in order to have a virtual distribution system that may be used to protect rights of various participants in electronic commerce or other electronic facilitated transactions. (Abstract; Ginter)

None of the references, however, explicitly disclose document encryption key encrypted with the public key associated with said rendering device. Olsen et al. in analogous art, however, disclose document encryption key encrypted with the public key associated with said rendering device. (Page 4, paragraph 54; ...a public key system is used to cipher the video decryption keys, ...) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al., Fung et al., Arima and Ginter to include encrypting document encryption key associated with the requested digital content with the public key associated with said digital secure repository. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Olsen et al. (Page 5, paragraph 55) in order to protect the keys during transmission from Content Distribution Portal to the Rendering Device.

As per claims 28 and 29:

Okamato et al. teach a method for storing digital content from a rendering device onto a storage device, the method comprising the following steps:

if storing is allowed according to the rights stored in said digital secure repository, receiving the respective document encryption key encrypted with the respective public key of all rendering devices registered in said digital secure repository, and storing the

encrypted keys together with said encrypted digital content on said storage device. (Col. 3, lines 64-67 and Col. 6, lines 49-56 Col. 7, lines 23-34)

Okamoto et al. further disclose a communication means between the distribution server and the user device and checking distribution condition by comparing the number of digital data; of which the same consumer registered in the history data is authorized to receive the distribution, and the distribution condition information. (Col. 6, lines 28-35). In addition, Okamoto et al. teaches encrypting means for encrypting the decryption key using a key that is created based on the media ID received from the user device.

Okamato et al. do not explicitly disclose establishing a connection from said rendering device to a digital secure repository; requesting from said digital secure repository digital content rights for specified digital content; document encryption key encrypted with the respective public key of all rendering devices; and said digital secure repository being associated with a user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content so as to allow said user to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring additional authorization from an external authority.

Fung et al. in analogous art, however, disclose

establishing a connection from said rendering device to a digital secure repository; (Page 1, paragraph 8, ...each client is associated with a universal mobile ID...)

requesting from said digital secure repository digital content rights for specified digital content. (Page 2, paragraph 15)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. to include establishing a connection from said rendering device to a digital secure repository; requesting from said digital secure repository digital content rights for specified digital content. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Fung et al. (Page 2, paragraph 14) in order to assemble the digital material which is send to the client device by using the access information which is contained in the Universal Mobile ID.

Both references do not explicitly disclose said digital secure repository being associated with a user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content so as to allow said user to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring additional authorization from an external authority.

Arima in analogous art, however discloses a storing unit that is being associated with said user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content on an authorized

rendering device in accordance with the access rights stored in said digital secure repository without requiring addition authorization from an external authority. (Page 3, paragraph 30; Page 4, paragraph 46)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. and Fung et al. to include a digital secure repository being associated with said user independently of a particular user device and storing access rights to said digital content granted to said user by a provider and a list of authorized rendering devices on which said user is allowed to render said digital content on an authorized rendering device in accordance with the access rights stored in said digital secure repository without requiring addition authorization from an external authority. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Arima (Abstract) in order to create a storing unit to store the digital contents ordered by a customer and creating a list for transmission to a player terminal and a transmitter that sends content selected by a customer to another player terminal. This way, the digital content is accessed by authorized customer and is transmitted to one or more player terminals registered as authorized terminals.

In addition, Arima further discloses a sales center server has a storage for storing information on the website accessed by the user terminal and information on digital contents. The sales center has a function of accepting a purchase request for digital contents from the user and accessing the server having the customer's digital contents rack as a delivery destination. (Page 3, paragraph 32)

None of the references explicitly disclose a digital secure repository being accessible to said user independently of said provider. Ginter in analogous art, however, discloses a digital secure repository being accessible to said user independently of said provider. (Col. 33, lines 10-15) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Okamoto, Fung and Arima with Ginter in order to have a virtual distribution system that may be used to protect rights of various participants in electronic commerce or other electronic facilitated transactions. (Abstract; Ginter)

None of the references, however, explicitly disclose document encryption key encrypted with the respective public key of all rendering devices. Olsen et al. in analogous art, however, disclose document encryption key encrypted with the respective public key of all rendering devices. (Page 4, paragraph 54; ...a public key system is used to cipher the video decryption keys, ...) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al., Fung et al., Arima and Ginter to include encrypting document encryption key associated with the requested digital content with the public key associated with said digital secure repository. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Olsen et al. (Page 5, paragraph 55) in order to protect the keys during transmission from Content Distribution Portal to the Rendering Device.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay SG

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER